

DEVICE AND METHOD FOR DATA PROCESSING AND RECORDING MEDIUM

Patent number: JP2001094552
Publication date: 2001-04-06
Inventor: MORINAGA TAKEO
Applicant: SONY CORP
Classification:
- **International:** H04L9/18; G06F12/14; H04L9/08
- **European:**
Application number: JP19990267262 19990921
Priority number(s): JP19990267262 19990921

Abstract not available for JP2001094552

Data supplied from the **esp@cenet** database - Worldwide

BEST AVAILABLE COPY

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2001-94552

(P2001-94552A)

(43)公開日 平成13年4月6日(2001.4.6)

(51)Int. Cl.⁷

識別記号

F I

テ-マ-ド(参考)

H 0 4 L 9/18

G 0 6 F 12/14 3 2 0 B 5B017

G 0 6 F 12/14 3 2 0

H 0 4 L 9/00 6 5 1 5J104

H 0 4 L 9/08

6 0 1 C

審査請求 未請求 請求項の数7

O L

(全16頁)

(21)出願番号 特願平11-267262

(22)出願日 平成11年9月21日(1999.9.21)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 森永 剛男

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100082131

弁理士 稲本 義雄

Fターム(参考) 5B017 AA06 BA07 BB02 BB03 CA06 CA16

5J104 AA12 AA16 EA02 EA15 JA04

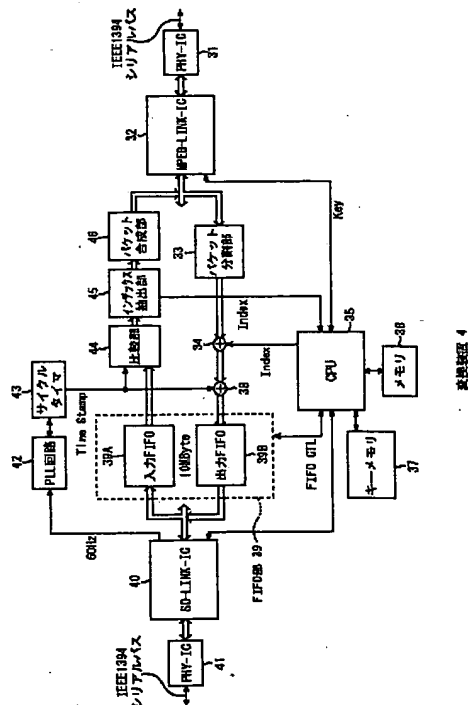
NA02 NA32 PA05

(54)【発明の名称】 データ処理装置およびデータ処理方法、並びに記録媒体

(57)【要約】

【課題】 デジタルコンテンツを違法なコピーから保護するとともに、DTCP(Digital Transmission Content Protection)の規格外のDVCRで記録する。

【解決手段】 DTCPの規格に適合した変換装置4では、MPEGリンクIC32において、デジタルCSチューナからの暗号化TSパケットに含まれている、暗号化および復号に用いるキーが抽出され、CPU35は、そのキーを、それを特定するためのインデックスと対応付けて、キーマモリ37に記憶させる。また、パケット分割部33では、暗号化TSパケットが、DVCRで記録可能なDIFブロックに変換され、演算器34では、そのDIFブロックの、キーが含まれていた位置に、そのキーに対応付けられたインデックスが付加される。そして、その結果得られるDIFブロックが、外部のDVCRに出力されて記録される。



【特許請求の範囲】

【請求項1】 所定のキーを用いて暗号化されたデータである暗号化データを処理するデータ処理装置であって、
前記暗号化データに含まれている前記キーを抽出するキー抽出手段と、
前記キーを、それを特定するためのインデックスと対応付けて記憶する記憶手段と、
前記暗号化データを、所定フォーマットのデータに変換する第1のフォーマット変換手段と、
前記所定フォーマットのデータの、前記キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加手段と、
前記インデックスが付加された前記所定フォーマットのデータを、外部に出力する第1の出力手段と、
外部から供給される前記所定フォーマットのデータから、前記インデックスを抽出するインデックス抽出手段と、
前記所定フォーマットのデータを、元のフォーマットの前記暗号化データに変換する第2のフォーマット変換手段と、
前記暗号化データの、前記インデックスが含まれていた位置に、そのインデックスに対応付けられた前記キーを付加するキー付加手段と、
前記キーが付加された前記暗号化データを、外部に出力する第2の出力手段とを含むことを特徴とするデータ処理装置。

【請求項2】 前記暗号化データは、トランスポートストリームであることを特徴とする請求項1に記載のデータ処理装置。

【請求項3】 前記所定フォーマットのデータは、D I F (Digital Interface) フォーマットのデータであることを特徴とする請求項1に記載のデータ処理装置。

【請求項4】 前記第1の出力手段は、前記暗号化データがコピーが許可されたものであるかどうか、または外部に接続された前記所定フォーマットのデータを受信する装置の仕様によって、前記所定のフォーマットのデータの出力を制限することを特徴とする請求項1に記載のデータ処理装置。

【請求項5】 前記第1の出力手段は、前記所定フォーマットのデータを出力するときに、そのデータについてのコピーを制御するためのコピー制御情報を操作することを特徴とする請求項1に記載のデータ処理装置。

【請求項6】 所定のキーを用いて暗号化されたデータである暗号化データを処理するデータ処理方法であって、
前記暗号化データに含まれている前記キーを抽出するキー抽出ステップと、
前記キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、

前記暗号化データを、所定フォーマットのデータに変換する第1のフォーマット変換ステップと、
前記所定フォーマットのデータの、前記キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、
前記インデックスが付加された前記所定フォーマットのデータを、外部に出力する第1の出力ステップと、
外部から供給される前記所定フォーマットのデータから、前記インデックスを抽出するインデックス抽出ステップと、
前記所定フォーマットのデータを、元のフォーマットの前記暗号化データに変換する第2のフォーマット変換ステップと、
前記暗号化データの、前記インデックスが含まれていた位置に、そのインデックスに対応付けられた前記キーを付加するキー付加ステップと、
前記キーが付加された前記暗号化データを、外部に出力する第2の出力ステップとを含むことを特徴とするデータ処理方法。

【請求項7】 所定のキーを用いて暗号化されたデータである暗号化データを、コンピュータに処理させるためのプログラムが記録されている記録媒体であって、
前記暗号化データに含まれている前記キーを抽出するキー抽出ステップと、
前記キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、
前記暗号化データを、所定フォーマットのデータに変換する第1のフォーマット変換ステップと、
前記所定フォーマットのデータの、前記キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、
前記インデックスが付加された前記所定フォーマットのデータを、外部に出力する第1の出力ステップと、
外部から供給される前記所定フォーマットのデータから、前記インデックスを抽出するインデックス抽出ステップと、
前記所定フォーマットのデータを、元のフォーマットの前記暗号化データに変換する第2のフォーマット変換ステップと、
前記暗号化データの、前記インデックスが含まれていた位置に、そのインデックスに対応付けられた前記キーを付加するキー付加ステップと、
前記キーが付加された前記暗号化データを、外部に出力する第2の出力ステップとを含むプログラムが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データ処理装置およびデータ処理方法、並びに記録媒体に関し、特に、IE

を伝送し、規格外の記録装置等でも、その記録を行うことができるようにするデータ処理装置およびデータ処理方法、並びに記録媒体に関する。

【0002】

【従来の技術】例えば、シリアルバス規格の1つであるIEEE(Institute of Electrical and Electronics Engineers)1394規格による通信は、データのアイソクロナス(isochronous)転送を行うことができることから、画像や音声といったリアルタイムで再生する必要のあるデジタルデータの転送に適しており、さらに、近年におけるマルチメディア通信の要請もあって、大きく注目されている。

【0003】ところで、デジタルビデオデータやデジタルオーディオデータ等のデジタルコンテンツは、その画質や音質を劣化させることなく、何度もコピーすることができるため、その著作権者等を違法なコピーから保護する必要がある。

【0004】そこで、本件出願人であるソニー株式会社を含む5社によって、IEEE1394シリアルバスを介して接続した装置どうしの間で、デジタルコンテンツを伝送するときの、そのデジタルコンテンツを保護するための規格として、5CDTCP(Five Company Digital Transmission Content Protection)(以下、適宜、DTCPという)が定められた。

【0005】DTCPでは、コピーフリーでないデジタルコンテンツの伝送に先立って、受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツを復号するようになっている。

【0006】DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、その暗号化されたデジタルコンテンツが、そこに含まれるキーを用いて復号される。

【0007】ここで、DTCPによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化されたデジタルコンテンツ(以下、適宜、暗号化コンテンツという)に含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。なお、本明細書中においては、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。

【0008】

【発明が解決しようとする課題】以上から、例えば、デジタルCS(Communication Satellite)チューナで受信したデジタルコンテンツを、IEEE1394シリアルバスを介して、コピー制御情報を正しく取り扱えない規格外のDVCR(Digital Video Tape Recorder)等で記録することはできない。

【0009】しかしながら、今後は、デジタルCSチューナで受信したデジタルコンテンツを、IEEE1394シリアルバスを介して、DVCRに伝送して録画するような利用形態に対するニーズが増加していくことが予想される。

【0010】また、デジタルCSチューナが出力する暗号化コンテンツを、DVCRで、そのまま録画すれば、デジタルコンテンツを違法なコピーから保護することができるが、録画した暗号化コンテンツを視聴することはできない。即ち、従来においては、DVCRで記録した暗号化コンテンツを再生し、デジタルCSチューナに入力して、その復号を行うのは困難であった。

【0011】本発明は、このような状況に鑑みてなされたものであり、デジタルコンテンツを違法なコピーから保護するとともに、規格外のDVCR等で記録すること等ができるようにするものである。

【0012】

【課題を解決するための手段】本発明のデータ処理装置は、暗号化データに含まれているキーを抽出するキー抽出手段と、キーを、それを特定するためのインデックスと対応付けて記憶する記憶手段と、暗号化データを、所定フォーマットのデータに変換する第1のフォーマット変換手段と、所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加手段と、インデックスが付加された所定フォーマットのデータを、外部に出力する第1の出力手段と、外部から供給される所定フォーマットのデータから、インデックスを抽出するインデックス抽出手段と、所定フォーマットのデータを、元のフォーマットの暗号化データに変換する第2のフォーマット変換手段と、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加するキー付加手段と、キーが付加された暗号化データを、外部に出力する第2の出力手段とを含むことを特徴とする。

【0013】暗号化データは、トランスポートストリームとすることができる。

【0014】所定フォーマットのデータは、DIF(Digital Interface)フォーマットのデータとすることができる。

【0015】第1の出力手段には、暗号化データがコピーが許可されたものであるかどうか、または外部に接続された所定フォーマットのデータを受信する装置の仕様

によって、所定のフォーマットのデータの出力を制限させることができる。また、第1の出力手段には、所定フォーマットのデータを出力するときに、そのデータについてのコピーを制御するためのコピー制御情報を操作させることができる。

【0016】本発明のデータ処理方法は、暗号化データに含まれているキーを抽出するキー抽出ステップと、キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、暗号化データを、所定フォーマットのデータに変換する第1のフォーマット変換ステップと、所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、インデックスが付加された所定フォーマットのデータを、外部に出力する第1の出力ステップと、外部から供給される所定フォーマットのデータから、インデックスを抽出するインデックス抽出ステップと、所定フォーマットのデータを、元のフォーマットの暗号化データに変換する第2のフォーマット変換ステップと、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加するキー付加ステップと、キーが付加された暗号化データを、外部に出力する第2の出力ステップとを含むことを特徴とする。

【0017】本発明の記録媒体は、暗号化データに含まれているキーを抽出するキー抽出ステップと、キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、暗号化データを、所定フォーマットのデータに変換する第1のフォーマット変換ステップと、所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、インデックスが付加された所定フォーマットのデータを、外部に出力する第1の出力ステップと、外部から供給される所定フォーマットのデータから、インデックスを抽出するインデックス抽出ステップと、所定フォーマットのデータを、元のフォーマットの暗号化データに変換する第2のフォーマット変換ステップと、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加するキー付加ステップと、キーが付加された暗号化データを、外部に出力する第2の出力ステップとを含むプログラムが記録されていることを特徴とする。

【0018】本発明のデータ処理装置およびデータ処理方法、並びに記録媒体においては、暗号化データに含まれているキーが抽出され、そのキーが、それを特定するためのインデックスと対応付けて記憶される。さらに、暗号化データが、所定フォーマットのデータに変換され、その所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスが付加されて、外部に出力される。一方、外部から供給さ

れる所定フォーマットのデータから、インデックスが抽出され、その所定フォーマットのデータが、元のフォーマットの暗号化データに変換される。そして、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーが付加されて、外部に出力される。

【0019】

【発明の実施の形態】図1は、本発明を適用したデジタル衛星放送受信システムの一実施の形態の構成例を示している。

【0020】図示せぬデジタル衛星放送局から放送されてくるデジタル衛星放送波は、アンテナ1で受信され、デジタルCSチューナ2に供給される。デジタルCSチューナ2は、DTCFに準拠した仕様を有し、アンテナ1から供給される信号から、所定の周波数帯域の受信信号を検波、復調し、MPEG(Moving Picture Experts Group)トランスポートストリームとする。さらに、デジタルCSチューナ2では、そのトランスポートストリームを構成するTSパケット(Transport Streamパケット)のうち、所定の1つのチャンネルのものが抽出され、その抽出されたTSパケットに含まれる、MPEG2エンコードされたビデオデータやオーディオデータが、MPEG2デコードされる。そして、そのデコードの結果得られたビデオデータまたはオーディオデータは、モニタ3に供給され、それぞれ画像として表示または音声として出力される。

【0021】また、デジタルCSチューナ2では、トランスポートストリームから、1チャンネル以上のTSパケットが抽出され、DTCFに準拠した方式で暗号化される。そして、その暗号化されたTSパケット(以下、適宜、暗号化TSパケット)は、IEEE1394シリアルバスを介して、変換装置4に供給される。

【0022】ここで、変換装置4は、IEEE1394シリアルバスを介して、デジタルCSチューナ2との間で、デジタルコンテンツのやりとりをする場合、DTCFに準拠した通信を行うようになっている。従って、デジタルCSチューナ2および変換装置4は、いずれも、相互認証を行った後、時間変化するキーを用いて、デジタルコンテンツを暗号化し、その結果得られる暗号化コンテンツに、暗号化に用いたキーを含めて、IEEE1394シリアルバス上に出力するようになっている。

【0023】変換装置4では、デジタルCSチューナ2からの暗号化TSパケットが、SD(Standard density)規格のDIF(Digital Interface)ブロックにフォーマット変換され、IEEE1394シリアルバスを介して、DVCR5に供給される。DV(Digital Video)機器であるDVCR5では、変換装置4からのDIFブロックが、図示せぬデジタルビデオテープに記録される。

【0024】ここで、DIFフォーマットについては、例えば、HD Digital VCR Conferenceにおいてまとめら

れたSpecification of Consumer Use Digital VCRs等に、その詳細が記載されている。

【0025】さらに、DVCR5では、デジタルビデオテープに記録されたDIFブロックが再生され、IEEE1394シリアルバスを介して、変換装置4に供給される。変換装置4では、DVCR5からのDIFブロックが、元の暗号化TSパケットにフォーマット変換され、IEEE1394シリアルバスを介して、デジタルCSチューナ2に供給される。デジタルCSチューナ2では、変換装置4からの暗号化TSパケットが、そこに含まれるキーを用いて復号され、さらにMPEGデコードされる。そして、そのデコードの結果得られたビデオデータまたはオーディオデータは、モニタ3に供給され、それぞれ画像として表示または音声として出力される。

【0026】次に、図2は、図1のデジタルCSチューナ2の構成例を示している。

【0027】アンテナ1がデジタル衛星放送波を受信することにより出力する受信信号は、フロントエンド部12に供給されるようになっている。

【0028】フロントエンド部12は、アンテナ1からの受信信号の復調等を行い、トランスポートストリームを得て、デスクランブラ13に供給する。デスクランブラ13は、フロントエンド部12からのトランスポートストリームにかけられているスクランブルを解き、スイッチ14に供給する。スイッチ14は、デスクランブラ13から供給されるトランスポートストリームを選択し、DEMUX(デマルチプレクサ)15に出力する。

【0029】DEMUX15は、CPU21の制御の下、スイッチ14から供給されるトランスポートストリームから、所定のチャンネルのTSパケットを抽出し、AVデコーダ16に供給するようになっている。AVデコーダ16は、CPU21の制御の下、DEMUX15からのTSパケットを、MPEG(Moving Picture Experts Group)デコードし、その結果得られるビデオデータおよびオーディオデータを、OSD(On Screen Display)処理部17に出力する。OSD処理部17では、CPU21の制御の下、所定の必要な画像(例えば、音量や、選択されているチャンネル等の表示)が、AVデコーダ16からのビデオデータに重畳され、D/A(Digital/Analog)コンバータ18に出力される。D/Aコンバータ18は、OSD処理部17が出力するデジタルコンテンツ(ここでは、ビデオデータおよびオーディオデータ)をD/A変換することにより、アナログ信号とし、例えば、モニタ3等に出力する。

【0030】以上のようにして、デジタル衛星放送として放送されてくるデジタルコンテンツは、モニタ3において表示等される。

【0031】一方、デジタル衛星放送として放送されてくるデジタルコンテンツを記録する場合には、スイッチ14は、デスクランブラ13からのトランスポート

ストリームを選択して、リンクIC(LINK Integrated Circuit)20に供給する。リンクIC20は、CPU21の制御の下、IEEE1394シリアルバスのレイヤ構造におけるリンク層の処理を行う他、スイッチ14からのトランスポートストリームを、DTCFに準拠して暗号化する。即ち、リンクIC20は、トランスポートストリームを、約30秒ごとに変更される8バイトのキーを用いて暗号化し、さらに、キーを、そのキーによって暗号化した最初のTSパケットの直前の位置等に挿入(付加)することにより、暗号化TSパケットとする。そして、リンクIC20は、この暗号化TSパケットを、アイソクロナス(Isochronous)パケットに配置して、ファイIC(PHY IC)19に供給する。ファイIC19は、リンクIC20からのアイソクロナスパケットを、IEEE1394シリアルバスを介して、変換装置4に、アイソクロナス転送する。

【0032】以上のようにして、デジタル衛星放送として放送されてくるデジタルコンテンツとしてのTSパケットは、IEEE1394シリアルバスを介して、変換装置4に供給され、変換装置4において、DIFブロック等への変換その他の処理が施された後、IEEE1394シリアルバスを介して、DVCR5に供給されて記録される。

【0033】次に、上述のようにしてDVCR5で記録されたデジタルコンテンツを再生する場合においては、DVCR5では、そのデジタルコンテンツとしてのDIFブロックが再生され、IEEE1394シリアルバスを介して、変換装置4に供給される。変換装置4では、DVCR5からのDIFブロックに対して、TSパケット等への変換その他の処理が施される。さらに、変換装置4では、TSパケットが配置されたアイソクロナスパケットが構成され、IEEE1394シリアルバスを介して、デジタル衛星チューナ2にアイソクロナス転送される。

【0034】デジタル衛星チューナ2では、ファイIC19において、変換装置4からのTSパケット(暗号化TSパケット)が配置されたアイソクロナスパケットが受信され、リンクIC20に供給される。リンクIC20は、CPU21の制御の下、ファイIC19からのアイソクロナスパケットに配置された暗号化TSパケットを、そこに付加されている(含まれている)キーを用いて復号し、スイッチ14に供給する。スイッチ14は、リンクIC20からのTSパケットを選択して、DEMUX15に出力し、以下、DEMUX15、AVデコーダ16、OSD処理部17、およびD/Aコンバータ18において、上述した場合と同様の処理が施され、DVCR5で記録されたデジタルコンテンツとしての画像および音声は、モニタ3から出力される。

【0035】なお、リンクIC20は、ファイIC19から受信したパケットが、AVデータ(ビデオデータ、オーディオデータ)が配置されたものである場合には、そのパケットを、スイッチ14に出力する。また、リン

クIC20は、ファイIC19から受信したバケットが、コマンドが配置されたものである場合には、そのバケットを、CPU21に出力する。

【0036】また、CPU21は、メモリ22に記憶されたプログラムを実行することで、DEMUX15、AVデコーダ16、およびOSD処理部17を制御するとともに、IEEE1394シリアルバスのレイヤ構造におけるトランザクション層やシリアルバス管理(Serial Bus Management)の処理等を行う。

【0037】さらに、メモリ22は、CPU21に、DEMUX15、AVデコーダ16、およびOSD処理部17の制御や、トランザクション層およびシリアルバス管理の処理を行わせるためのプログラム(ファームウェア)を記憶している。また、メモリ22は、CPU21の動作上必要なデータを、一時記憶するようにもなっている。

【0038】次に、図3は、図1の変換装置4の構成例を示している。

【0039】ファイIC31は、IEEE1394シリアルバスを介して、デジタルCSチューナ2との間でやりとりされるデータの送受信を行うようになっている。即ち、ファイIC31は、IEEE1394シリアルバスを介して、デジタルCSチューナ2から送信されてくるバケットを受信し、MPEGリンクIC(MPEG-LINK-IC)32に供給するとともに、MPEGリンクIC32からのバケットを、IEEE1394シリアルバスを介して、デジタルCSチューナ2に送信するようになっている。

【0040】MPEGリンクIC32は、ファイIC31から供給される暗号化TSバケットを、バケット分割部33に供給するとともに、その暗号化TSバケットに付加されているキー(Key)を抽出し、CPU35に供給するようになっている。さらに、MPEGリンクIC32は、CPU35から供給されるキーを受信し、そのキーを、バケット合成部46から供給される暗号化TSバケットの、元の位置に付加(挿入)して、ファイIC31に供給するようになっている。

【0041】バケット分割部33は、MPEGリンクIC32からの暗号化TSバケットを、DIFブロックに変換するようになっている。

【0042】即ち、TSバケットは、そのまのフォーマットでは、DVCR5で記録することができないため、バケット分割部33において、DVCR5で記録することのできるDIFブロックに変換されるようになっている。

【0043】具体的には、DIFブロックは、図4(A)に示すように、80バイトで構成される。そして、その先頭の3バイトには、DIFブロックを識別するためのID(Identification)が配置され、残りの77バイトに、データが配置される。

【0044】一方、TSバケットは、一般に、188バ

イトで構成される。このため、バケット分割部33は、TSバケットを分割し、図4(B)に示すように、3つのDIFブロックに分けて配置することで、TSバケットをDIFブロックに変換する。

【0045】即ち、3つのDIFブロックの先頭の3バイトには、図4(A)に示したように、IDが配置される。さらに、3つのDIFブロックとも、3バイトのIDの後には、ダミーデータとしての13バイトの0が配置される。そして、3つのDIFブロックにおいて、ダミーデータの後の残りの64バイトに、188バイトのTSバケットが分割されて配置される。但し、図4の実施の形態では、3つのDIFブロックのうち、最初と2番目のDIFブロックには、188バイトのTSバケット(TRS)のうちの64バイトずつが配置されるが、最後のDIFブロックには、188バイトのTSバケットの残りの60バイトと、後述するサイクルタイム43が出力する4バイトのタイムスタンプ(TS(Time Stamp))とが配置される。

【0046】図3に戻り、演算器34は、バケット分割部33からのDIFブロックに、CPU35から供給されるインデックスを付加し、演算器38に出力するようになっている。即ち、CPU35は、MPEGリンクIC32から供給される、暗号化TSバケットに付加されているキーに対して、現在の日時等の、キーを特定することのできるインデックスを対応付け、そのインデックスを、演算器34に供給するようになっており、演算器34は、そのようにしてCPU35から供給されるインデックスを、そのインデックスに対応付けられたキーが付加されていた暗号化TSバケットが配置されたDIFブロックに付加するようになっている。従って、DIFブロックに付加されたインデックスによれば、MPEGリンクIC32がバケット分割部33に出力する暗号化TSバケットのシーケンスのどの位置に、そのインデックスに対応付けられたキーが配置されていたかを認識することができる。

【0047】ここで、DIFブロックは、図5に示すように、150ブロックを1つのユニットとして、DVCR5等のDV機器に伝送され、その150のDIFブロックのうち、先頭のDIFブロック(ヘッダセクション(Header section)と呼ばれる)を除く149ブロックが、デジタルビデオテープの1トラックに記録される。演算器34では、図5に示すようなユニットを構成するDIFブロックに配置された暗号化TSバケットを復号するのに用いるキーに対応付けられたインデックスが、例えば、図5においてV0で示すDIFブロック等の、所定のDIFブロックに配置される。

【0048】再び、図3に戻り、CPU35は、メモリ36に記憶されたプログラムを実行することで、各種の処理を行うようになっている。

【0049】即ち、CPU35は、上述したように、M

PEGリンクIC32から供給される、暗号化TSパケットに付加されているキーに対して、インデックスを対応付け、そのインデックスを、演算器34に供給する。さらに、CPU35は、その対応付けたインデックスとキーの組を、キーメモリ37に供給して記憶させる。また、CPU35は、インデックス抽出部45からインデックスを受信し、そのインデックスに対応付けられているキーを、キーメモリ37から読み出して、MPEGリンクIC32に供給する。さらに、CPU35は、FIFO(First In First Out)部39およびSDリンクIC(SD-LINK-IC)40を制御する。

【0050】メモリ36は、CPU35に、上述したような処理を行わせるためのプログラムを記憶している。さらに、メモリ36は、CPU35の動作上必要なデータを一時記憶するようになっている。キーメモリ37は、CPU35から供給されるインデックスとキーメモリの組を一時記憶するようになっている。なお、DTC Pでは、上述したように、TSパケットの暗号化/復号に用いられる8バイトのキーが、約30秒ごとに更新されるため、DVCR5において1時間の記録を行うごとに、キーメモリ37では、約9800バイト分のキーと、それらのキーに対応付けられたインデックスが記憶されることになる。

【0051】演算器38は、サイクルタイマ43が出力するタイムスタンプを、演算器34が出力するDIFブロックに付加し、FIFO部39に出力するようになっている。

【0052】FIFO部39は、再生時に、SDリンクIC40が出力するDIFブロックを一時記憶し、比較部44に出力する入力FIFO39Aと、記録時に、演算器38が出力するDIFブロックを一時記憶し、SDリンクIC40に出力する出力FIFO39Bとから構成されている。

【0053】ここで、トランスポートストリームのデータレートは、一般に、4Mbps(Bit Per Second)である。一方、DVCR5が、SD規格に準拠したものであるとすると、その記録レートは25Mbps程度である。従って、TSパケットを変換したDIFブロックを、特に時間軸制御することなく、DVCR5で記録したのでは、デジタルビデオテープの多くの記録領域が使用されないこととなり、記録効率が悪い。そこで、変換装置4では、入力FIFO39Aまたは出力FIFO39Bにおいて、DIFブロックを一時記憶することにより、その時間軸伸張または時間軸圧縮をそれぞれ行い、トランスポートストリームのデータレートと、DVCR5の記録レートとの間の差を吸収して、DVCR5において、効率の良い記録を行うことができるようになっている。

【0054】なお、出力FIFO39Bでは、DIFブロックの記録時に、DIFブロックが一時記憶されることにより、その時間軸圧縮が行われるが、この時間軸圧縮に

より、TSパケット間の元の時間間隔が損なわれる。従って、再生時には、その損なわれた時間間隔を復元する必要があるが、そのために、演算器38において、DIFブロックにタイムスタンプが付加される。

【0055】以上のように、トランスポートストリームのデータレートと、DVCRの記録レートとの差を吸収して、効率の良い記録を行い、かつそのようにして記録されたデータを正常に再生する方法については、本件出願人が先に出願した特開平11-74796号公報(特願平9-231943号)に、その詳細が開示されている。

【0056】SDリンクIC40は、CPU35の制御の下、FIFO部39の出力FIFO39Bに記憶されたDIFブロックを読み出し、アイソクロナスパケットに配置して、ファイIC(PHY-IC)41に供給するようになっている。また、SDリンクIC40は、ファイIC41から供給されるアイソクロナスパケットを受信し、そこに配置されているDIFブロックをFIFO部39の入力FIFO39Aに供給するようになっている。さらに、SDリンクIC40は、例えば、60Hzのクロックを、PLL(PHase Lock Loop)回路42に供給するようになっている。

【0057】ファイIC41は、SDリンクIC40からのアイソクロナスパケットを、IEEE1394シリアルケーブルを介して、DVCR5に、アイソクロナス転送し、また、DVCR5から、IEEE1394シリアルバスを介してアイソクロナス転送されてくるアイソクロナスパケットを受信し、SDリンクIC40に供給するようになっている。

【0058】PLL回路42は、SDリンクIC40からのクロックに同期して、サイクルタイマ43に所定のクロックを出力するようになっている。サイクルタイマ43は、PLL回路42からのクロックをカウントし、そのカウント値を、タイムスタンプとして、演算器38および比較部44に供給するようになっている。

【0059】比較部44は、入力FIFO39Aに記憶されているDIFブロックに付加されているタイムスタンプと、サイクルタイマ43が出力するタイムスタンプとを比較し、サイクルタイマ43の出力と一致するタイムスタンプが付加されているDIFブロックを、入力FIFO39Aから読み出して、インデックス抽出部45に出力するようになっており、これにより、上述したように、時間軸圧縮によって損なわれたTSパケット間の時間間隔が復元されるようになっている。

【0060】インデックス抽出部45は、比較部44からのDIFブロックに付加されているインデックスを抽出し、CPU35に出力するとともに、そのDIFブロックを、パケット合成部46に出力するようになっている。

【0061】パケット合成部46は、図4(B)に示し

たように、3つのDIFブロックに分割して配置されたTSパケットを、その3つのDIFブロックを合成することで元に戻し、MPEGリンクIC32に出力するようになっている。

【0062】次に、図6のフローチャートを参照して、変換装置4において、デジタルコンテンツをDVCR5で記録するときに行われる処理について説明する。

【0063】デジタルコンテンツをDVCR5で記録する場合においては、上述したように、デジタルCSチューナ2から、IEEE1394シリアルバスを介し、変換装置4に対して、暗号化TSパケットが配置されたアイソクロナスパケットが送信され、そのアイソクロナスパケットは、ファイIC31で受信される。ファイIC31は、受信したアイソクロナスパケットを、MPEGリンクIC32に出力し、MPEGリンクIC32は、アイソクロナスパケットを受信すると、ステップS1において、そのアイソクロナスパケットに配置された暗号化TSパケットを、パケット分割部33に供給する。

【0064】パケット分割部33では、ステップS1において、MPEGリンクIC32からの暗号化TSパケットを分割し、図4で説明したように、3つのDIFブロックに変換して、演算器34に出力する。

【0065】そして、ステップS2に進み、CPU35において、パケット分割部33が出力したDIFブロックに分割された暗号化TSパケットに、キーが付加されていたかどうか判定される。即ち、MPEGリンクIC32は、上述したように、ファイIC31から受信した暗号化TSパケットに、キーが付加されている場合には、そのキーを抽出して、CPU35に供給するようになっており、CPU35は、ステップS2において、そのようにして、MPEGリンクIC32からキーが供給されてきたかどうかによって、パケット分割部33が出力したDIFブロックに分割された暗号化TSパケットに、キーが付加されていたかどうかを判定する。

【0066】ステップS2において、暗号化TSパケットに、キーが付加されていないと判定された場合、演算器34は、その暗号化TSパケットを変換したDIFブロックを、演算器38に出力し、ステップS3およびS4をスキップして、ステップS5に進む。

【0067】また、ステップS2において、暗号化TSパケットに、キーが付加されていると判定された場合、ステップS3に進み、CPU35は、そのキー、即ち、MPEGリンクIC32から供給されるキーに、インデックスを対応付け、そのインデックスを、演算器34に出力する。演算器34は、CPU35からのインデックスを、パケット分割部33からのDIFブロックに付加し、演算器38に出力する。

【0068】そして、ステップS4に進み、CPU35は、演算器34に出力したインデックスと、それに対応付けたキーとの組を、キーメモリ37に供給して記憶さ

せ、ステップS5に進む。

【0069】ステップS5では、演算器38において、演算器34が出力するDIFブロックに、サイクルタイム43が出力するタイムスタンプが付加され、ステップS6に進み、FIFO部39の出力FIFO39Bに出力される。出力FIFO39Bでは、演算器38からのDIFブロックが記憶される。そして、出力FIFO39Bに記憶されたDIFブロックは、CPU35の制御にしたがって読み出され、SDリンクIC40およびファイIC41を経由し、IEEE1394シリアルバスを介して、DVCR5に供給されて記憶される。

【0070】ステップS6の処理後は、ステップS7に進み、次の暗号化TSパケットが、IEEE1394シリアルバスを介して、デジタルCSチューナ2から伝送されてきたかどうか判定され、伝送されてきたと判定された場合、その暗号化TSパケットは、ファイIC31で受信され、MPEGリンクIC32を介して、パケット分割部33に供給される。そして、ステップS1に戻り、以下、同様の処理が繰り返される。

【0071】また、ステップS7において、次の暗号化TSパケットが、IEEE1394シリアルバスを介して、デジタルCSチューナ2から伝送されてきていないと判定された場合、即ち、記録対象の暗号化TSパケットの伝送が終了した場合、処理を終了する。

【0072】以上のように、DTCPの規格に適合した変換装置4において、デジタルCSチューナ2からの暗号化TSパケットに含まれている、暗号化および復号に用いるキーを抽出し、そのキーを、それを特定するためのインデックスと対応付けて記憶する一方、暗号化TSパケットを、DVCR5で記録可能なDIFブロックに変換し、そのDIFブロックの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加して、外部のDVCR5に出力するようにしたので、デジタルコンテンツを違法なコピーから保護するとともに、DTCPの規格外のDVCR5で記録することができ

【0073】即ち、デジタルCSチューナ2と変換装置4とを接続するIEEE1394シリアルバスにおいても、変換装置4とDVCR5とを接続するIEEE1394シリアルバスにおいても、そこを転送されるデータは暗号化されており、従って、デジタルコンテンツを違法なコピーから保護することができる。さらに、デジタルCSチューナ2が出力するデジタルコンテンツは、DTCPの規格に適合した変換装置4を介して、DVCR5に供給されるので、DTCPの規格に適合していないDVCR5において、デジタルCSチューナ2が出力するデジタルコンテンツを記録することができる。

【0074】次に、図7のフローチャートを参照して、変換装置4において、上述のようにして、DVCR5で記録されたデジタルコンテンツを再生するときに行わ

れる処理について説明する。

【0075】DVCR5で再生されたDIFブロックは、IEEE1394シリアルバスを介して、変換装置4に転送され、変換装置4では、ファイIC41において、DVCR5からのDIFブロックが受信され、SDリンクIC40に供給される。SDリンクIC40は、ファイIC41からのDIFブロックを、順次、FIFO部39の入力39Aに供給して記憶させる。

【0076】そして、ステップS11において、比較部44は、入力FIFO39Aに記憶されている、最も古いDIFブロックに付加されているタイムスタンプと、サイクルタイマ43から供給されるタイムスタンプとを比較し、それらが等しいかどうかを判定する。ステップS11において、DIFブロックに付加されているタイムスタンプと、サイクルタイマ43のタイムスタンプとが等しくないと判定された場合、ステップS11に戻る。

【0077】また、ステップS11において、DIFブロックに付加されているタイムスタンプと、サイクルタイマ43のタイムスタンプとが等しいと判定された場合、ステップS12に進み、比較部44は、そのタイムスタンプが付加されているDIFブロックと、そのDIFブロックの一部が配置されている暗号化TSパケットの他の一部が配置されているDIFブロックを、入力FIFO39Aから読み出し、インデックス抽出部45に出力する。

【0078】インデックス抽出部45は、ステップS13において、比較部44からのDIFブロックに、インデックスが付加されているかどうかを判定し、付加されていない場合、そのDIFブロックを、パケット合成部46に出力し、ステップS14およびS15をスキップして、ステップS16に進む。

【0079】また、ステップS13において、比較部44からのDIFブロックに、インデックスが付加されていると判定された場合、ステップS14に進み、インデックス抽出部45は、そのDIFブロックに付加されているインデックスを抽出し、CPU35に出力して、ステップS15に進む。

【0080】ステップS15では、CPU35は、インデックス抽出部35からのインデックスと対応付けられているキーを、キーメモリ37から読み出し、MPEGリンクIC32に出力する。

【0081】そして、ステップS16に進み、パケット合成部46において、インデックス抽出部45からのDIFブロックが、元の暗号化TSパケットに合成され、MPEGリンクIC32に出力される。

【0082】MPEGリンクIC32は、CPU35からキーが供給されてこない場合には、パケット合成部46からの暗号化TSパケットを、ファイIC31に出力し、また、CPU35からキーが供給されてきた場合には、パケット合成部46からの暗号化TSパケットに、

そのキーを付加して、ファイIC31に出力する。これにより、ファイIC31からは、記録時に、デジタルCSチューナ2から転送されてきたときと同じ状態の暗号化TSパケットが、IEEE1394シリアルバスを介して、デジタルCSチューナ2に転送され、デジタルCSチューナ2では、このようにして、DVCR5から変換装置4を介して転送されてくるデジタルコンテンツが、上述したようにしてモニタ3に表示される。

【0083】ステップS16の処理後は、ステップS17に進み、入力FIFO39Aに、DIFブロックが、まだ記憶されているかどうか判定される。ステップS17において、入力FIFO39Aに、DIFブロックが、まだ記憶されていると判定された場合、ステップS11に戻り、以下、同様の処理が繰り返される。

【0084】また、ステップS17において、入力FIFO39Aに、DIFブロックが記憶されていないと判定された場合、即ち、DVCR5の再生が終了し、その再生によって得られたDIFブロックをすべて処理した場合、処理を終了する。

【0085】以上のように、変換装置4において、外部のDVCR5で再生されたDIFブロックから、インデックスを抽出するとともに、そのDIFブロックを、暗号化TSパケットにフォーマット変換し、その変換後の暗号化TSパケットの、抽出されたインデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加して、外部のデジタルCSチューナ2に出力するようにしたので、デジタルCSチューナ2では、上述したようにして、その暗号化TSパケットを復号し、デジタルコンテンツとしての画像や音声を再生することができる。

【0086】なお、上述の場合には、変換装置4において、デジタルCSチューナ2からの暗号化TSパケットを復号せずに処理するようにしたが、暗号化TSパケットは、一旦復号してから処理することも可能である。即ち、暗号化TSパケットは、MPEGリンクIC32において、暗号化TSパケットに含まれるキーを用いて復号してから、DIFブロックへの変換等を行い、SDリンクIC40において、そのDIFブロックを暗号化してから、DVCR5に記録するようにすることが可能である。この場合も、デジタルコンテンツを違法なコピーから保護するとともに、DTCPの規格外のDVCR5で記録することができる。

【0087】但し、この場合、再生時には、SDリンクIC40において、DVCR5からの、暗号化されたDIFブロックを復号してから、TSパケットへの変換等を行い、MPEGリンクIC32において、そのTSパケットを、キーを用いて暗号化（DTCPの規格に準拠した暗号化）してから、デジタルCSチューナ2に出力する必要がある。

【0088】また、DTCPにおいては、コピーを制御

するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)が規定されている。EMIが00B(Bは、その前の値が2進数であることを表す)である場合は、デジタルコンテンツがコピーフリーのもの(Copy-freely)であることを表し、EMIが01Bである場合には、デジタルコンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、EMIが10Bである場合は、デジタルコンテンツが、1度だけコピーして良いもの(Copy-one-generation)であることを表し、EMI

が11Bである場合には、デジタルコンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【0089】変換装置4(図3)のSDリンクIC40では、そこに入力されるDIFブロックから、上述のようなEMIを検出し、そのEMIに基づいて、DIFブロックを、外部のDVCR5に出力するかどうかを制限するようにすることが可能である。即ち、例えば、EMIが、Copy-freelyである場合以外は、DTCPの規格外の装置であるDVCR5には、DIFブロックを出力

しないようにすること等が可能である。

【0090】さらに、SDリンクIC40には、EMIを、DTCPの規格に反しない範囲で操作させることが可能である。即ち、例えば、EMIが、Copy-one-generationを表す10Bとなっている場合において、DIFブロックを、外部のDVCR5に出力するときには、そのEMIを、No-more-copiesを表す01Bに変更することが可能である。なお、EMIの操作は、変換装置4に入力されたデジタルコンテンツが、その入力された端子以外の端子から出力される場合にのみ行うようにする

ことが可能である。

【0091】また、変換装置4では、CPU35において、ファイIC41と、IEEE1394シリアルバスを介して接続される装置の種類(装置が何であるか)や、メーカーを確認するようにして、あらかじめ設定された種類やメーカーの装置以外には、DIFブロックを出力しないようにすることが可能である。この場合、違法コピーを目的として製作された装置へのDIFブロックの出力を防止することが可能となる。

【0092】次に、図8は、本発明を適用したデジタル衛星放送受信システムの他の実施の形態の構成例を示している。なお、図中、図1における場合と対応する部分については、同一の符号を付してある。即ち、図8のデジタル衛星放送受信システムは、デジタルCSチューナ2および変換装置4に替えて、デジタルCSチューナ51が設けられている他は、図1における場合と同様に構成されている。

【0093】デジタルCSチューナ51は、図1のデジタルCSチューナ2と変換装置4とを一体的にした機能を有している。

【0094】即ち、図9は、図8のデジタルCSチューナ51の構成例を示している。なお、図中、図2のデジタルCSチューナ2と対応する部分については、同一の符号を付してある。即ち、図9のデジタルCSチューナ51は、バケット分割部61、バケット合成部62、およびキーメモリ63が新たに設けられている他は、図2のデジタルCSチューナ2と基本的に同様に構成されている。

【0095】バケット分割部61は、図3のバケット分割部33と同様に、スイッチ14が出力するTSバケットを、DIFブロックにフォーマット変換し、リンクIC20に出力するようになっている。バケット合成部62は、図3のバケット合成部46と同様に、リンクIC20が出力するDIFブロックを、元のTSバケットにフォーマット変換し、スイッチ14に供給するようになっている。キーメモリ63は、図3のキーメモリ37と同様に、CPU21から供給されるキーとインデックスとの組を記憶するようになっている。

【0096】なお、図9のメモリ22には、図2で説明したようなプログラムの他、デジタルCSチューナ51を、変換装置4として機能させるためのプログラムも記憶されており、従って、CPU21は、変換装置4が行う処理も行うようになっている。

【0097】以上のように構成されるデジタルCSチューナ51では、図2における場合と同様にして、デジタル衛星放送として放送されてくるデジタルコンテンツが、モニタ3に表示等される。

【0098】一方、デジタル衛星放送として放送されてくるデジタルコンテンツを記録する場合には、スイッチ14は、デスクランブラ13からのトランスポートストリームを、バケット分割部61に供給し、バケット分割部61では、トランスポートストリームを構成するTSバケットが、DIFブロックにフォーマット変換され、リンクIC20に供給される。

【0099】リンクIC20では、CPU21の制御の下、DIFブロックに分割されたTSバケットが、図2における場合と同様にして、時間変化するキーを用いて暗号化される。さらに、リンクIC20では、その暗号化結果から、キーが抽出され、CPU21に供給される。CPU21は、リンクIC20からのキーに、インデックスを対応付け、キーメモリ63に記憶させる。さらに、CPU21は、キーに対応付けたインデックスを、リンクIC20に供給し、リンクIC20では、そのインデックスが、図3の演算器34における場合と同様にして、DIFブロックに付加される。その後、リンクIC20では、CPU21の制御の下、DIFブロックに対するタイムスタンプの付加や、DIFブロックの時間軸圧縮等が行われ、ファイIC19に出力される。ファイIC19は、リンクIC20からのDIFブロックを、IEEE1394シリアルバスを介して、DVCR5に転

送り、これにより、DVCR5では、そのDIFブロックが記録される。

【0100】次に、上述のようにして記録されたDIFブロックが、DVCR5で再生されると、その再生されたDIFブロックは、IEEE1394シリアルバスを介して、デジタルCSチューナ51に転送される。デジタルCSチューナ51では、ファイIC19において、DVCR5からのDIFブロックが受信され、リンクIC20に供給される。リンクIC20では、DIFブロックの時間軸伸張等が行われ、その後、DIFブロックに付加されているインデックスが抽出される。このインデックスは、リンクIC20からCPU21に供給され、CPU21は、リンクIC20からインデックスを受信すると、そのインデックスに対応付けられているキーを、キーメモリ3から読み出し、リンクIC20に供給する。リンクIC20では、CPU21からのキーを用いて、DIFブロックに分割されているTSパケットが復号され、パケット合成部62に出力される。

【0101】パケット合成部62では、リンクIC20からのDIFブロックが、元のTSパケットに合成され、スイッチ14に供給される。そして、以下、スイッチ14、DEMUX15、AVデコーダ16、OSD処理部17、およびD/Aコンバータ18において、上述した場合と同様の処理が施され、これにより、DVCR5で記録されたデジタルコンテンツとしての画像および音声、モニタ3から出力される。

【0102】次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアとしての変換装置4やデジタルCSチューナ51に組み込まれているコンピュータ(図3のCPU35や、図9のCPU21が相当する)や、汎用のコンピュータ等にインストールされる。

【0103】そこで、図10を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる、そのプログラムが記録されている記録媒体について説明する。

【0104】プログラムは、図10(A)に示すように、コンピュータ101に内蔵されている記録媒体としてのハードディスク102や半導体メモリ103に予め記録しておくことができる。

【0105】あるいはまた、プログラムは、図10(B)に示すように、フロッピーディスク111、CD-ROM(Compact Disc Read Only Memory)112、MO(Magnetic optical)ディスク113、DVD(Digital Versatile Disc)114、磁気ディスク115、半導体メモリ116などの記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このような記録媒体は、い

わゆるパッケージソフトウェアとして提供することができる。

【0106】なお、プログラムは、上述したような記録媒体からコンピュータにインストールする他、図10(C)に示すように、ダウンロードサイト121から、デジタル衛星放送用の人工衛星122を介して、コンピュータ101に無線で転送したり、LAN(Local Area Network)、インターネットといったネットワーク131を介して、コンピュータ123に有線で転送し、コンピュータ101において、内蔵するハードディスク102などにインストールすることができる。

【0107】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理(例えば、並列処理あるいはオブジェクトによる処理)も含むものである。

【0108】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0109】次に、図11は、図10のコンピュータ101の構成例を示している。

【0110】コンピュータ101は、図11に示すように、CPU(Central Processing Unit)142を内蔵している。CPU142には、バス141を介して、入出力インタフェース145が接続されており、CPU142は、入出力インタフェース145を介して、ユーザによって、キーボードやマウス等で構成される入力部147が操作されることにより指令が入力されると、それにしたがって、図10(A)の半導体メモリ103に対応するROM(Read Only Memory)143に格納されているプログラムを実行する。あるいは、また、CPU142は、ハードディスク102に格納されているプログラム、衛星122若しくはネットワーク131から転送され、通信部148で受信されてハードディスク102にインストールされたプログラム、またはドライブ149に装着されたフロッピーディスク111、CD-ROM112、MOディスク113、DVD114、若しくは磁気ディスク115から読み出されてハードディスク102にインストールされたプログラムを、RAM(Random Access Memory)144にロードして実行する。そして、CPU142は、その処理結果を、例えば、入出力インタフェース145を介して、LCD(Liquid Crystal Display)等で構成される表示部146に、必要に応じて出力する。

【0111】なお、本実施の形態では、本発明を、デジタル衛星放送を受信するデジタル衛星放送受信システムに適用した場合について説明したが、本発明は、その他、デジタルコンテンツを取り扱う装置に適用可能

である。

【0112】また、本明細書中におけるトランスポートストリームには、188バイトのTSパケットで構成されるストリームの他、そのTSパケットをデコードするのと同様の原理でデコードされる、例えば、米国のDirecTV社がDSS(Direct Satellite System)で用いている130バイトのパケットで構成されるストリーム等も含まれる。

【0113】

【発明の効果】以上の如く、本発明のデータ処理装置およびデータ処理方法、並びに記録媒体によれば、暗号化データに含まれているキーが抽出され、そのキーが、それを特定するためのインデックスと対応付けて記憶される。さらに、暗号化データが、所定フォーマットのデータに変換され、その所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスが付加されて、外部に出力される。一方、外部から供給される所定フォーマットのデータから、インデックスが抽出され、その所定フォーマットのデータが、元のフォーマットの暗号化データに変換される。そして、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーが付加されて、外部に出力される。従って、デジタルコンテンツを違法なコピーから保護して、所定フォーマットの形で記録、再生を行うことができる。

【図面の簡単な説明】

【図1】本発明を適用したデジタル衛星放送受信システムの一実施の形態の構成例を示すブロック図である。

【図2】図1のデジタルCSチューナ2の構成例を示すブロック図である。

【図3】図1の変換装置4の構成例を示すブロック図である。

【図4】図3のパケット分割部33の処理を説明するための図である。

【図5】図3の演算器34の処理を説明するための図である。

【図6】DVCR5で記録を行う場合の、図3の変換装置4の処理を説明するためのフローチャートである。

【図7】DVCR5で再生を行う場合の、図3の変換装置4の処理を説明するためのフローチャートである。

【図8】本発明を適用したデジタル衛星放送受信システムの他の実施の形態の構成例を示すブロック図である。

【図9】図8のデジタルCSチューナ51の構成例を示すブロック図である。

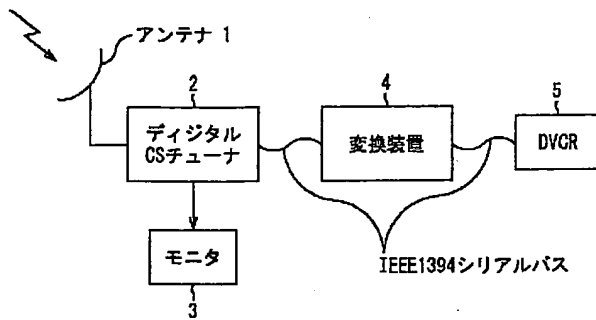
【図10】本発明を適用した記録媒体を説明するための図である。

10 【図11】図10のコンピュータ101の構成例を示すブロック図である。

【符号の説明】

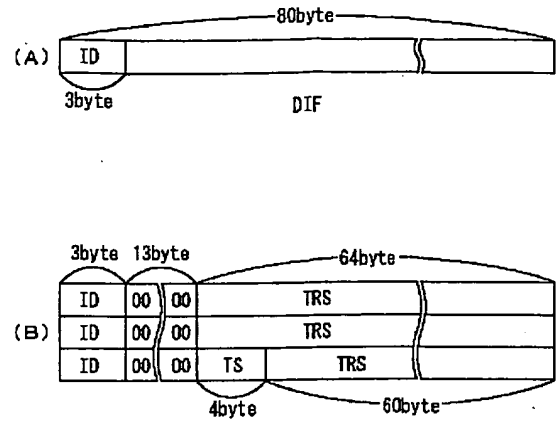
1 アンテナ, 2 デジタルCSチューナ, 3 モニタ, 4 変換装置, 5 DVCR, 12 フロントエンド部, 13 デスクランブラ, 14 スイッチ, 15 DEMUX, 16 AVデコーダ, 17 OSD処理部, 18 D/Aコンバータ, 19 ファイIC, 20 リンクIC, 21 CPU, 22 メモリ, 31 ファイIC, 32 MPEGリンクIC, 33 パケット分割部, 34 演算器, 35 CPU, 36 メモリ, 37 キーメモリ, 38 演算器, 39 FIFO部, 39A入力FIFO, 39B 出力FIFO, 40 SDリンクIC, 41 ファイIC, 42 PLL回路, 43 サイクルタイマ, 44 比較部, 45 インデックス抽出部, 46 パケット合成部, 51 デジタルCSチューナ, 61 パケット分割部, 62 パケット合成部, 63 キーメモリ, 101 コンピュータ, 102 ハードディスク, 103 半導体メモリ, 111 フロッピーディスク, 112 CD-ROM, 113 MOディスク, 114 DVD, 115 磁気ディスク, 116 半導体メモリ, 121ダウンロードサイト, 122 衛星, 131 ネットワーク, 141 バス, 142 CPU, 143 ROM, 144 RAM, 145 入出力インタフェース, 146 表示部, 147 入力部, 148 通信部, 149 ドライブ

【図1】

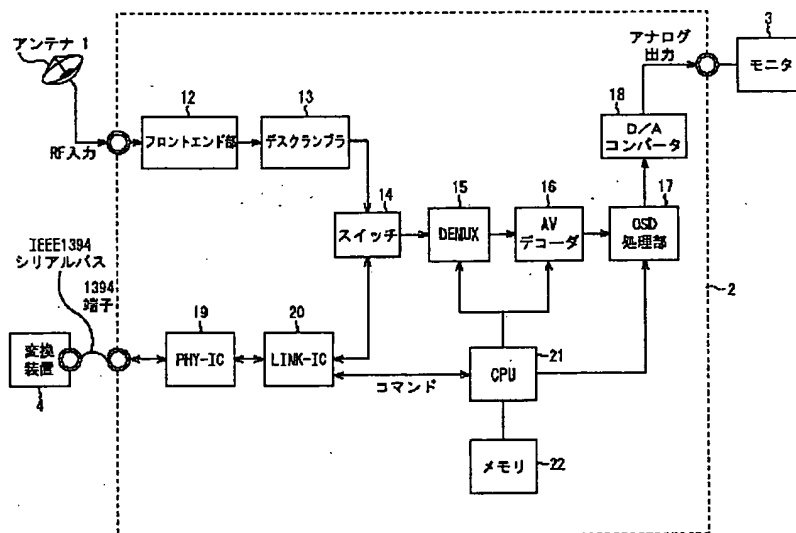


デジタル衛星放送受信システム

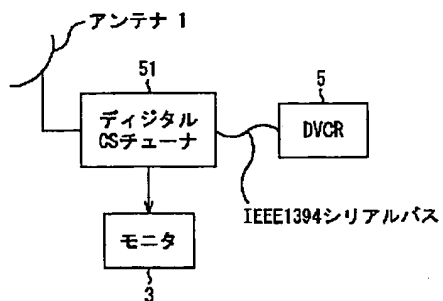
【図4】



【図2】

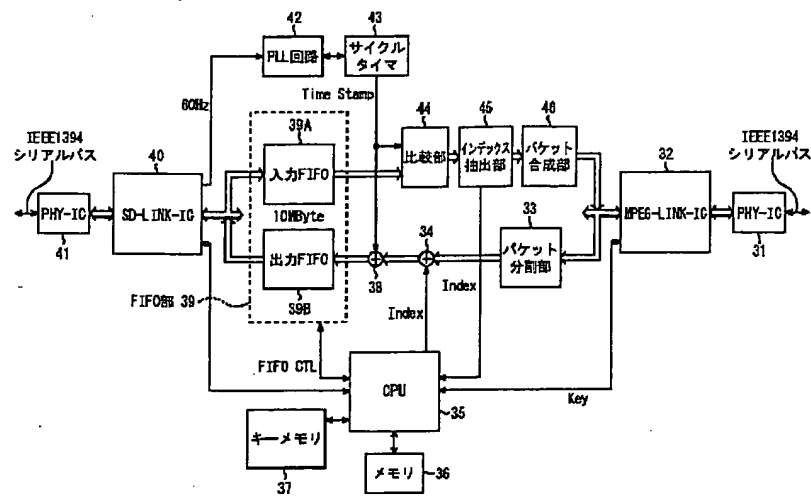


【図8】



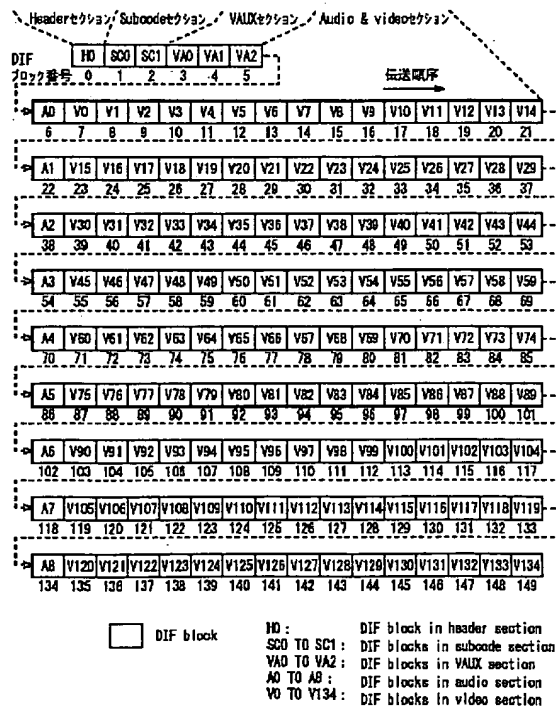
デジタル衛星放送受信システム

【図3】



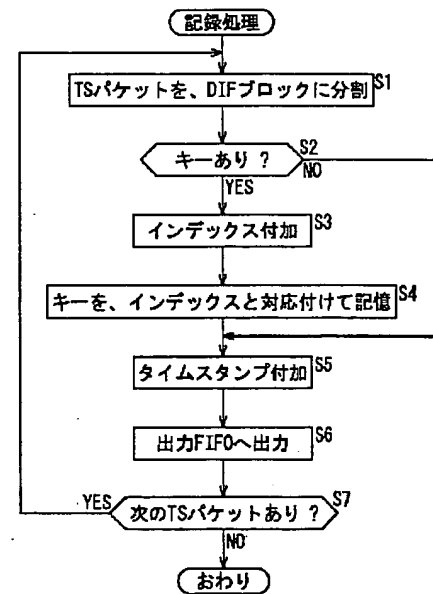
変換装置 4

【図5】

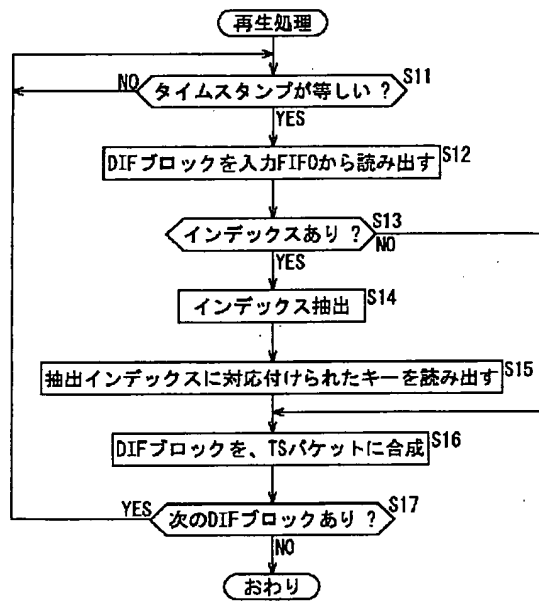


Transmission order of DIF blocks in a DIF sequence

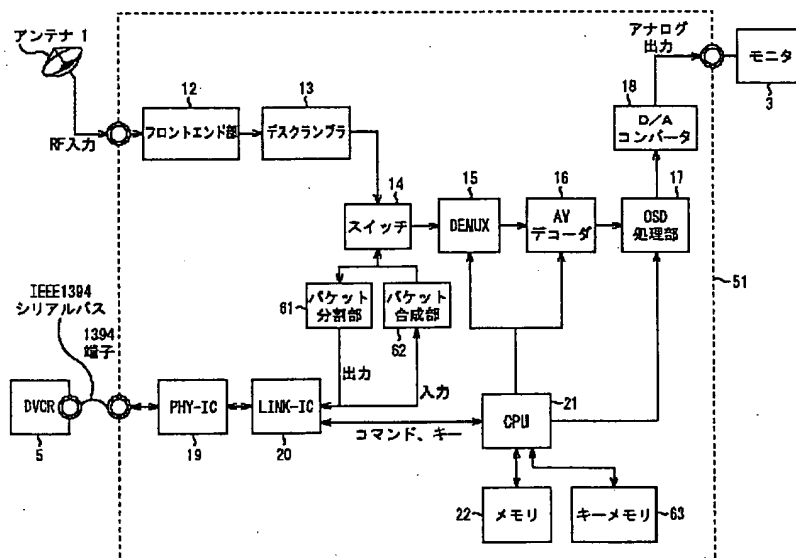
【図6】



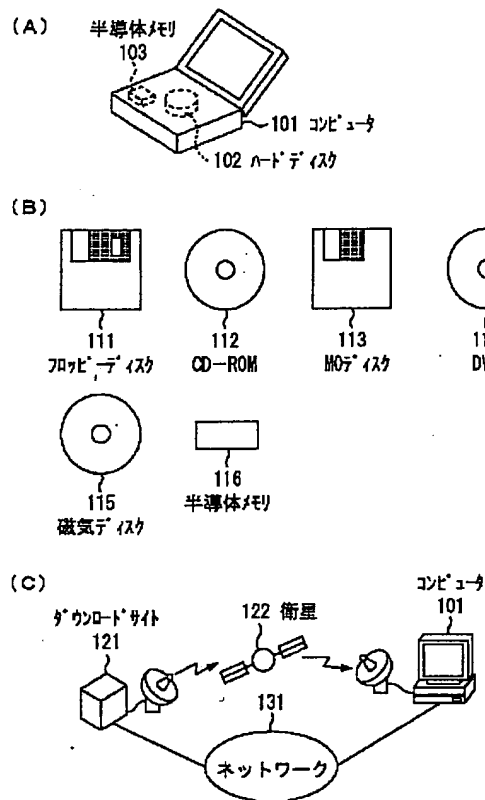
【図7】



【図9】



【図10】



【図11】

